What is claimed is:

1. A microprocessor comprising:

an identifier that identifies the microprocessor; and

embedded instructions for comparing a hash value, derived from the identifier and a key, to an expected hash value.

2. The microprocessor of claim 1 further comprising embedded instructions for producing a hash value that is a function of the identifier and a key.

3. The microprocessor of claim 2 wherein the identifier comprises a processor number.

4. The microprocessor of claim 3 wherein the embedded instructions comprise microcode.

5. The microprocessor of claim 4 wherein the key corresponds to an address for a web site.

6. The microprocessor of claim 5 wherein the expected hash value is derived from a key that corresponds to an address for a web site and a processor number.

7. A computer-readable medium having computer-executable instructions stored therein that, when executed by a microprocessor, cause an expected hash value, which is derived from a key and a first identifier for a computer system, to be compared with a hash value, which is derived from the key and a second identifier for a computer system.

8. The computer-readable medium of claim 7 further comprising computer-executable instructions stored therein that, when executed by a microprocessor, cause the result of that comparison to be communicated to an application.

9. The computer-readable medium of claim 8 wherein the application comprises a decryption program.

10. A server comprising:

a computer-readable medium having computer-executable instructions stored therein that, when executed by a microprocessor, cause an expected hash value, which is derived from a key corresponding to a web site and a first identifier for a computer system, to be compared with a hash value, which is derived from the key and a second identifier for a computer system.

11. The server of claim 10 wherein the computer-executable instructions comprise a decryption program and wherein the computer-readable medium further comprises computer-executable instructions stored therein that, when executed by a microprocessor, cause the result of that comparison to be communicated to the decryption program.

12. A method for confirming the identity of a computer system comprising:

transmitting a request from an application to a computer system to confirm the identity of the computer system, the request accompanied by a key and an expected hash value derived from that key and a first identifier for a computer system;

retrieving a second identifier that identifies the computer system;

generating a hash value derived from the second identifier and the key; and

comparing that hash value with the expected hash value.

13. The method of claim 12 wherein the application comprises a decryption program and wherein the method further comprises:

storing the result of the hash value comparison; and

forwarding that result to the decryption program.

14. The method of claim 13 wherein the first and second identifiers are each processor numbers.

15. The method of claim 14 wherein the key comprises a unique bit string that corresponds to a web site address.

16. The method of claim 13 further comprising returning a true response if the first and second processor numbers are identical, and returning a false response if the first and second processor numbers are not identical.

17. A method for binding an application to a computer system comprising:

periodically checking the identity of a computer system as it executes an application to ensure that the computer system is authorized to execute the application, such periodic checks performed by:

delivering to a microprocessor a key and an expected hash value, derived from the key and a first processor number for a computer system; and

instructing the microprocessor to compare that expected hash value to a hash value derived from that key and the processor number for the computer

system that is executing the program, then to return to the application the result of that comparison.

18. The method of claim 17 wherein the application comprises a decryption program.

19. The method of claim 18 wherein the instructions for requesting the hash value comparison are embodied in tamper resistant software.

20. A computer-readable medium having computer-executable instructions stored therein that, when executed by a microprocessor, cause the identity of a computer system to be periodically checked as it executes an application to ensure that the computer system is authorized to execute the application, such periodic checks performed by:

delivering to a microprocessor a key and an expected hash value, derived from the key and a first processor number for a computer system; and

instructing the microprocessor to compare that expected hash value to a hash value derived from that key and the processor number for the computer system that is executing the program, then to return to the application the result of that comparison.

21. A method for binding the execution of encrypted content, and an accompanying decryption program, to a platform comprising:

transmitting to a computer system encrypted content, and an accompanying decryption program, the decryption program comprising a hash value and instructions for performing periodic checks on the identity of any

computer system that executes the decryption program, as that program is executed; and

performing those periodic identity checks by comparing the hash value delivered by the decryption program with a second hash value derived at least in part from an identifier for the computer system that executes the program.

22. The method of claim 21 wherein the hash value is derived from the processor number for the computer system that received from a web site the encrypted content and accompanying decryption program, and a bit string that corresponds to an URL for that web site.

23. The method of claim 22 wherein the computer system delivered the hash value to the web site before the web site delivered the encrypted content, and accompanying decryption program, to the computer system.

24. The method of claim 23 wherein the decryption program, including the instructions for performing the periodic identity checks, are embodied in tamper resistant software.